12-2018

Risk-Based Performance Metrics for Critical Infrastructure Protection? A Framework for Research and Analysis

Eric F. Taquechel

Marina Saitgalina
Old Dominion University, msaitgal@odu.edu

Original Publication Citation

Taquechel, Eric F. & Marina Saitgalina. Risk-based performance metrics for critical infrastructure protection? A framework for research and analysis. *Homeland Security Affairs* 14, Article 8 (December 2018). https://www.hsaj.org/articles/14699

HOMELAND SECURITY AFFAIRS
(https://www.hsaj.org/)

The Journal of the NPS Center for Homeland Defense and Security

Risk-Based Performance Metrics for Critical Infrastructure Protection? A Framework for Research and Analysis

Posted on December 2018

By Eric F. Taquechel & Marina Saitgalina

Abstract

Measuring things that do not occur, such as “deterred” or “prevented” terrorist attacks, can be difficult. Efforts to establish meaningful risk-based performance metrics and performance evaluation frameworks based on such metrics, for government agencies with counterterrorism missions, are arguably in a nascent state. However, by studying program theory, logic models, and performance evaluation theory, as well as studying how risk, deterrence, and resilience concepts may be leveraged to support antiterrorism efforts, one may propose a framework for a logic model or other performance evaluation approach. Such a framework may integrate these concepts to help proxy performance measurement for agencies with prevention and/or deterrence missions. This effort would not be without challenges.

Suggested Citation

Taquechel, Eric F. & Marina Saitgalina. “Risk-Based Performance Metrics for Critical Infrastructure Protection? A Framework for Research and Analysis.” *Homeland Security Affairs* 14, Article 8 (December 2018). https://www.hsaj.org/articles/14699 (https://www.hsaj.org/articles/14699)

Introduction

Performance measurement is critical to effective government, as it is intended to help improve public management and program outcomes.[1] Performance measurement, when properly done, operationalizes abstract goals, specifies policies, and informs management decisions. However, certain government functions and missions are difficult to measure.[2] Specifically, adversarial missions such as antiterrorism and law enforcement which center on prevention and/or deterrence may make useful performance evaluation challenging. Therefore, this essay will examine considerations for performance evaluation frameworks that may be useful for assessing agency prevention or deterrence missions. Intended audiences of this research include program managers, performance analysts, policy evaluators, budget analysts, and Congressional budget oversight committees.

Context

Risk management is a critical aspect of CIKR (critical infrastructure/key resources) protection efforts for the Department of Homeland Security (DHS). Risk management may encompass efforts to deter attacks thus reducing threat, protect CIKR thus reducing vulnerability, and increase CIKR resilience

thereby reducing consequence. It may also entail simultaneous execution of such efforts. Threat is the likelihood that an attack occurs, and that likelihood includes attacker intent and attacker capability, estimated as probabilities.[3] Vulnerability is the likelihood an attack is successful given that it is attempted[4]. Consequence is the effects of an attack.[5]

Together, these three elements—threat, vulnerability, and consequence—can be combined to form a quantitative approximation of terrorist attack risk. Since performance metrics are also critical to effective government,[6] the status of efforts to create meaningful performance evaluation systems for antiterrorism programs that specifically leverage risk metrics warrants review.

Importance

The New Public Management (NPM) framework of public administration focuses on outcomes instead of inputs and processes.[7] This focus has been reaffirmed in the context of exploration of homeland security performance metrics. For example, some analysts claim that outcome-oriented performance management has increasingly supplanted output and process management.[8]

If we believe that the outcome-oriented focus of NPM is still relevant today, despite the alternative theoretical framework of New Public Service (NPS) which prioritizes citizen engagement and inclusiveness (c.f. Denhardt & Denhardt, 2015, p. 32), we must explore how to measure homeland security enterprise outcomes. However, as budgets continue to be constrained, efficiency is just as important as effectiveness. Therefore, a more holistic approach to agency performance evaluation should adopt measures that include resource inputs, activities, and accomplishments (outputs).

Evaluating public agency resource inputs and activities helps with budgeting control and accountability. As agencies make “resource input” decisions in proposed budgets, those agencies can exercise some form of control over their programs. Control is one purpose of budgeting; it ensures tax dollars are used to accomplish budgeted objectives.[9] Historically, “object budgeting,” or the itemization of expenditures on specific objects, served a control purpose.[10] Therefore, the budgeting objective was to control line-item expenditures.

Also, budgeting serves a management/efficiency approach.[11] After strategic priorities and objectives are determined, budgeting helps achieve efficiencies in attaining those priorities by allocating limited financial resources. Thus, understanding the outputs that certain resource inputs and activities support helps agencies manage efforts to achieve their strategic objectives more efficiently. Since budgeting also serves a planning purpose,[12] agencies must look at outcome trends to help justify out-year budgets, in support of long- term effectiveness. Existing “planning, programming, budgeting and execution” (PPBE) guidance may help agencies connect the dots between strategic agency priorities, resource needs, and resource constraints. For example, DHS’ FY2006 Congressional Budget Justification includes an overview of the goals of PPBE, which acknowledge fiscal constraints.[13]

Therefore, good fiscal management in public agency antiterrorism program administration warrants consideration of resource inputs, activities, accomplishments, and outcomes, with appropriate supporting metrics. Developing a theoretical framework integrating such considerations could be useful for agencies with prevention or deterrence-oriented missions. In that spirit, exploration of considerations for an appropriate risk-based performance measurement framework seems appropriate, so public agencies with CIKR protection responsibilities can continuously refine program execution and budgeting efforts.

Research Goals

The following research questions can be posed to help shape and inform the research in support of such a framework.

1. What is the current state of literature that might inform performance evaluation frameworks for agencies with antiterrorism mandates, specifically including protecting CIKR?
2. What are potential challenges to advancing performance evaluation frameworks, specifically with respect to incorporating risk terminology and risk theory?

Such a research effort might explore areas of the literature including risk theory, performance measurement theory, program evaluation theory, and law enforcement metrics. Additionally, such effort may benefit from a review of ideas on how to integrate concepts from risk management, particularly deterrence, risk analysis, and resilience theory, into performance evaluation frameworks. We propose ideas on how to integrate these concepts at the end of the essay, in an appendix.

Expected Research Benefits

If we believe public agencies with CIKR protection responsibilities should continuously strive to improve program execution and budgeting efforts, such agencies could benefit from conceptual frameworks to develop and refine risk-based performance metrics to help defend their budgets. Research shows that motivation for using performance metrics includes assessing effectiveness and tracking expenditure allocation.[14] Additionally, academics continue to explore ways to use quantitative data to promote better agency effectiveness and contain costs.[15]

Literature Review

Existing Literature

Performance Measurement & Logic Model Theory

McLaughlin and Jordan identify two purposes for measuring program performance: communicating value to others/accountability, and program improvement.[16] However, what are specific ways to facilitate these purposes? Greenfield et al. discuss the theory of logic models. Logic models are conceptual frameworks to communicate visually a simplified representation of a program's activities, outputs, customers, and outcomes to internal and external audiences, and they serve as planning tools.[17] Therefore, logic models are one framework for managing communications and program improvement as advocated by McLaughlin and Jordan. Moreover, both McLaughlin and Jordan and Greenfield et al. offer detailed guidance to help logic- model developers ensure those models are valuable. For instance, they recommend ensuring that if intermediate agency outcomes are achieved, the end-state outcomes will reasonably follow.[18] This speaks to establishing causation or correlation between elements of the logic model.

Risk & CIKR Protection – Theory

There is much research in the theoretical and applied aspects of risk management for homeland security missions. More specifically, there is a genre of literature that deals with risk theory as applied to CIKR protection. Taquechel and colleagues summarize some of the notable work in this literature in addition to offering their own insights.[19]

Taquechel and colleagues offer that the intent- probability component of threat can be influenced by agency activities that deter attacks by reducing vulnerability and/or consequence to attack, and such deterrence efforts can be quantified. Furthermore, they argue that CIKR vulnerabilities to exploitation by weapons of mass destruction (WMD) or illicit materiel/personnel transfer can be modeled as logic networks, with implications for how analysts assess vulnerability or more specifically "exploitation susceptibility" of such networks. Additionally, Taquechel and colleagues propose that grants might be administered to help CIKR rebuild after an attack, but distributed as a pre-attack mitigation measure, based on network analysis of supply- chain resilience. Other work in the areas of deterrence theory, risk analysis, and resilience includes that of Alderson et al., Cox, Dighe et al., Kahan et al., Jenelius et al., Lebow and Stein, Lewis, Morral and Jackson, and Vugrin et al.[20]

Incorporating risk theory into performance evaluation poses an opportunity to discuss deterrence theory and adaptive adversary considerations as possible "moderator variables" influencing the nexus between intermediate and end-state agency outcomes. Deterrence theory is multifaceted, but it can succinctly be described as the principle of "when an actor discourages aggression towards another actor, with the intended outcome that the former never has to respond to aggressive action by the latter."[21] Furthermore, adaptive adversaries are those that can change their behavior or characteristics in response to prevention, protection, response, or recovery efforts.[22] Adaptive adversary considerations and deterrence quantification are important for CIKR risk analysis,[23] and Savitz et al. reinforce the idea of considering reactions of "other parties" in performance measurement.[24] Therefore, the perceived effect of changes in adversary intent upon threat- reduction metrics could be a valuable component of a logic model framework to integrate risk metrics with antiterrorism program performance evaluation.

Anderson et al. claim that logic models help program managers map out "competing definitions of the determinants of a problem."[25] Since there are different theories about the underlying determinants of risk, in particular the ongoing debate over "static", probabilistic-based risk analysis vs the "dynamic" game theoretical/adaptive adversary approach espoused by the operations research community (c.f. Taquechel and Lewis, 2012, Taquechel, 2013), logic models may help visually conceptualize how both static and dynamic probabilities of attack could influence risk- reduction effectiveness metrics for various antiterrorism activities.

Program theory and "complicated interventions"

Showing causality or even correlation between prevention/deterrence-oriented homeland security activities and ultimate risk reduction outcomes may be challenging. Rogers discusses the idea of complicated vs. complex/emergent programs. Complicated programs are those with multiple components, whereas "complex" programs represent programs with "recursive causality" and tipping points.[26] Therefore, logic models to describe complex programs may have inherent nonlinearities. Furthermore, Rogers mentions that the external environment, characteristics of clients, and overlapping programs could cause overconfidence in correlation estimates.[27]

In risk parlance, resilience is the "ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption."[28] The definition of resilience also includes system recovery. Systems imply networks, and networks often display emergent phenomena.[29] Therefore, if DHS must defend networks of CIKR, and not just individual infrastructures, performance metrics that incorporate resilience or consequence reduction may need to account for network-emergent phenomena such as "self-organizing criticality", wherein systems optimize for efficiency but possibly to the detriment of resilience. This speaks to Rogers' claim of external influence on program performance, although network-emergent phenomena often result from internal, "self-organizing" aspects of network evolution. Nonetheless, this is a "complexity" consideration for program evaluation. Self-organized criticality may create a tipping point.

Applying performance measurement to programs that reduce consequence and increase resilience may be difficult. Specifically, Henstra claims that "one of the most formidable challenges facing local communities today is learning to apply the concepts and methods of performance measurement to disaster preparedness."[30] Cutter et al. add to the debate over this difficulty; they claim it is difficult to measure resilience in absolute terms and proxy variables may be needed.[31]

Another consideration in the literature is that there are different types of logic models used in program theory. For example, "pipeline" logic models show a linear progression from inputs to activities to outputs, whereas "outcome chain" logic models may demonstrate outcomes where initial activities were not considered, and "realist matrix" logic models may model how interventions work

differently for different groups in different situations.[32] If antiterrorism missions have inherent nonlinearities, especially when it comes to risk modeling, performance evaluators may benefit from different types of logic models.

Performance metrics in law enforcement and antiterrorism

Law enforcement metrics may inform development of counterterrorism metrics given the common "adversarial nature" of the two missions. Similarly, metric evaluation in law enforcement agencies can be challenging. For example, Braga and Bond discuss efforts to assess correlation between "hot-spot" policing activities and crime levels.[33] Deterrence is another influence upon risk metrics in law enforcement, as it is in antiterrorism. In theory, policing preemptively may deter criminal or terrorist activity. However, from a logic- model perspective, Brousselle and Champagne advise that logic analysis, the evaluation of a program's underlying theory using available scientific knowledge, needs to establish that the means correlate to the desired ends.[34] With deterrence theory, the notion that certain enforcement activities influenced the adversary's "intent" can be a theoretical exercise, without direct evidence of causation. This can make logic-model validation difficult.

Another takeaway from Braga and Bond's work is the importance of identifying special causal factors in a program with multiple dimensions.[35] Since risk reduction is theoretically achieved by threat-reduction activities, vulnerability- reduction activities, consequence- reduction activities, or a combination of the above, a performance-evaluation framework should allow "individual activity" effect isolation, as well as "simultaneously executed activity" effect analysis. Nicholson-Crotty et al. caution against excessive information aggregation; they claim multiple detailed measures of the same concept are often preferable to one aggregate measure.[36]

However, aggregation might be valuable for different aspects of risk metrics. For instance, Ayyub claims the primary basis for evaluating resilience should include both aggregate measures of systems resilience as well as "segregated performance" of individual system components.[37] If program managers want to model the effects of consequence-reducing activities upon residual risk (risk remaining after those activities are performed), they might consider both segregated consequence to individual CIKR, as well as aggregate network effects-based consequences to a CIKR system such as cascading failures. Keeney and Von Winterfeldt also advocate for metric aggregatibility, particularly with respect to whether program objectives are additive or multiplicative.[38] For instance, the availability of a radiological detection device is one metric, and the device detection accuracy is another. The two detection program objectives in this case are multiplicative rather than additive.[39] Since risk analysis may be quantitative, determining whether metrics should be additive or multiplicative may be crucial.

Additional work with logic models and risk metrics in the antiterrorism world includes evaluation of the effectiveness of the Global Nuclear Detection Architecture (GNDA), a federal program to minimize radiological and nuclear terrorism risk to the U.S. This work evaluated GDNA program goals, objectives, and activities, the goals here being to minimize individual components of the risk equation: threat, vulnerability, and consequence. Each goal had subordinate objectives.[40] This study also evaluated results exclusive of costs to lower these risk- equation components, instead saving those costs for cost-effectiveness analysis.[41]

Previous work on analyzing risk reduction metrics vs cost effectiveness also separated costs from the "utility functions" or what outcomes prospective attackers would stand to gain from successful attacks. However, like Hilliard et al., those costs were used for return on investment analysis of different government strategies to deter prospective attackers (c.f. Taquechel and Lewis, 2012; Taquechel, Hollan, and Lewis, 2015; Taquechel and Lewis, 2016). This also speaks to the concept of "metric aggregatibility" emphasized in other work; here it made sense to segregate cost from performance effectiveness metrics, but this may not always be true.

Art of the Possible?

It may be possible to address the "problem" of developing a framework for risk-based performance evaluation in antiterrorism missions that specifically involve CIKR protection. Creating a logic model that incorporates activities, accomplishments and outcomes of such missions, and supporting those logic- model elements with a variety of quantitative risk metrics, might advance solutions. Furthermore, it may be possible to evaluate the appropriate use of risk metrics based on their value in helping budget for an antiterrorism program, based on principles of line item/cost center accountability, efficiency, and/or overall program effectiveness. Moreover, such a logic model may be able to capture the effects of quantifiable deterrence and network effects upon risk metrics, as well as other considerations from this literature review.

Literature Gaps

In light of the two identified research goals, and given this snapshot of "art of the possible", a review of the literature identifies the following gaps. With respect to the first research goal, to our knowledge the literature does not explicitly discuss a theory or model of how antiterrorism activities, outputs, and outcomes might be organized within a performance- evaluation framework, with supporting quantitative risk metrics, perhaps broken down by each component of the risk equation (threat, vulnerability, consequence). Hilliard et al. (2015) specifically discussed nuclear weapon risk in what might be termed a "logic model" framework, but future work might be generalized to all CIKR risk.

With respect to the second research goal, the literature has gaps in several areas. First, despite the claims of Anderson and Savitz et al. that external influences must be accounted for and problems may have competing interpretations, to our knowledge the literature does not specifically explore how a

performance evaluation framework might reconcile multiple interpretations of the threat component of the risk equation, specifically the ongoing debate over probabilistic risk analysis vs. operations research/game theory (c.f. Taquechel & Lewis, 2012).

Second, the literature does not specifically discuss the challenge of how measurable adaptive-adversary influences on risk, possibly as a recursive mechanism of action, could be incorporated into a performance- evaluation framework. Furthermore, Taquechel and Lewis showed how deterrence effects of certain activities could be quantified and proposed how the effects of such activities were double-counted in revised risk equations.[42] Specifically, vulnerability- reduction activities at CIKR both deter, thus reducing threat, and reduce vulnerability, therefore "doubly" reducing risk. However, to our knowledge no literature has proposed how such accounting for risk reduction might inform a performance- evaluation framework.

Third, despite Henstra's and Cutter's efforts to explore performance metrics in the area of resilience, the literature does not specifically discuss how quantifiable network effects on system resilience could be incorporated into a performance- evaluation framework for agencies with CIKR protection responsibilities. Fourth, despite the ongoing debate in the literature regarding metric aggregatibility (c.f. Ayyub, Nicholson-Crotty, Braga & Bond, Keeney & Von Winterfeldt), to our knowledge the literature does not examine how vulnerability and exploitation potential of CIKR and networks comprised thereof, both in terms of individual and aggregate vulnerability or exploitation potential, might be incorporated into performance- evaluation frameworks.

Recommendations and Implications – Logic Model Framework Development

Recommendations

We recommend developing a logic- model framework that maps antiterrorism activities to outputs to outcomes. Outputs may include attacks prevented/deterred, compliance achieved, and damage minimized. Outcomes may entail residual risk, or risk remaining after activities are executed and outputs (risk that was reduced) are tabulated. Furthermore, the quantitative metrics for outputs might reflect different budgeting theories, for example as discussed in Hou (2006). Additionally, such a logic model might incorporate activities and metrics that account for the nonlinear and recursive effects of adaptive- adversary influence on CIKR risk, as well as the complexity of network effects upon vulnerability and consequence.

For instance, output metrics fashioned after the "responsibility center" or "line-item budgeting" approach might explore threat reduced by attacks deterred. Alternatively, metrics fashioned after the efficiency or performance-based budgeting approach might explore risk reduced, solely as a function of those threat-reducing activities, divided by time or cost spent executing those activities. As a third

option, output metrics fashioned after “effectiveness-based” or “rational-comprehensive” based budgeting may explore risk reduced, as a function only of threat-reducing activities, but omitting a cost/time denominator.

Our speculation is that activity metrics should reflect number of activities performed, and that output metrics should reflect quantified risk reduced. Furthermore, we speculate that outcome metrics should be quantified residual risk after activities are performed. Greenfield et al. claim in a notional logic model for a government injury-prevention program that the reduction in the incidence of sexual violence is considered an “end outcome” metric.[43] The end goal in this work seems to be minimized “residual violence.” More generally, they claim metrics associated with annual goals typically serve as indicators of a program’s *efforts* (our emphasis), whereas the intermediate and strategic goals (equivalent to outcomes) and their associated metrics are indicative of a program’s *effect* (our emphasis).[44] By that logic, antiterrorism activities might be considered efforts, whereas risk reduced and residual risk to CIKR might be the effects.

Implications and Constraints

Such a logic- model framework would assume that antiterrorism activities can be estimated to reduce quantitatively elements of risk. In other words, certain activities might be estimated to reduce threat through deterrence; other activities might be assumed to reduce vulnerability through increasing target security and law enforcement response capabilities; and yet other activities might be assumed to reduce consequence through response and recovery efforts.

The multiplicative effects of specific activities on multiple elements of the risk equation might be accounted for in a theoretical fashion, but this could make line-item budgeting difficult. However, activities that reduce multiple aspects of risk, e.g. through both deterring (reducing threat) and protecting CIKR (e.g., reducing vulnerability), might be thought as of “robust activities.” Furthermore, agency capabilities leveraged to execute those activities might be thought of as “robust capabilities,” something that certain agencies may value even if it made activity-based or line-item budgeting difficult. One theory is that goals, requirements, and metrics should be conceived more in terms of “capability envelopes” rather than particular scenarios.[45] However, in agencies where budgeting is closely linked to capabilities (e.g. aircraft, boats, specialized tactical units), especially capabilities that perform multiple missions, a logic- model approach based on activity performance and linkage to outcomes may be challenging if one objective is to inform budget development.

Fiscal Constraints

Allocation of performance requires outcome measures; whereas budgeting decisions require efficiency measures.[46] If an agency with antiterrorism mission-execution responsibilities is resource constrained, it may prefer only activity-based budgeting, here meaning budgeting for costs of executing a certain number of antiterrorism activities, without regard to output or outcome.

Conversely, if an agency focuses more on performance-based budgeting, it may prefer to adjust activity execution to reduce a certain amount of risk, or leave a certain amount of estimated residual risk. A modeled optimization solution could maximize risk reduction given an upper- bound constraint on resources.

Political Constraints

Some claim that outcome-based metrics are so general as to be meaningless for budgeting and accounting purposes.[47] Based on the approach proposed here, if residual risk outcome metrics are perceived as inefficacious for supporting line- item or efficiency-based budgeting, the literature would suggest that not even an antiterrorism program's effectiveness-based budgeting effort could realistically be supported by residual risk metrics.

As agencies develop and propose budgets in an environment where elected officials scrutinize agency- performance metrics, it may be difficult to justify funding based on a program-logic model that advocates risk reduction, even if elected officials like the principle of programs targeting quantitative risk reduction. Accountability for performance is sometime perceived as secondary compared to accountability for finances and for procedural fairness.[48] Therefore, even if a rigorous model linking activities to risk-reduction metrics is developed, expenditures on capability packages or activity execution may receive more scrutiny than expenditures incurred in aggregate to achieve stated risk reduction goals.

Another consideration is that performance standards can be derived from past performance or performance of similar agencies.[49] If politicians are not familiar with the evolving technical aspects of quantitative risk analysis and management, they may benchmark agency performance off previous performance or that of similar agencies, possibly to the detriment of what an agency is truly trying to achieve.

Technological Constraints

Models that optimize performance are subject to tradeoffs between rigor and simplicity. Any modeling effort that maps specific activity execution to quantitative risk- reduction metrics, slicing and dicing amongst the theoretical elements of risk (threat, vulnerability, consequence) may increase in cost as complexity increases. Greenfield et al. encourage determining correlation or causality in logic models[50]; but Savitz et al. claim that some metrics for one federal agency's antiterrorism mission might be inherently unreliable given the paucity of real-world terrorist attacks.[51]

Time constraints

Some agencies require models that support certain decisions to undergo a formal Verification, Validation, and Accreditation (VV&A) process. Such a process could require lots of analyst effort and financial support. Fortunately, model accreditation processes in some agencies may be tailored subject to resource constraints. Furthermore, the wicked problem approach may limit model effectiveness, absent sufficient time to develop such a model. Caudle (2005) argues that:

> *[t]he program logic model has one major drawback for homeland security in that it clearly targets programs, normally within an organization's control, as the unit of analysis…complex program logic models would be necessary for homeland security to reflect the interdependencies of many organizations and programs.*[52]

With this in mind, modeling the effects of Rogers' (2008) program "overlap" upon logic- model activities and metrics might increase the time needed to construct a valuable risk metric-based logic model for CIKR protection missions.

Conclusions

The research here suggests that efforts to establish meaningful risk-based performance evaluation models with risk metrics for use by agencies with counterterrorism missions are in a somewhat nascent state. However, we are optimistic that by continuing to study program theory, logic models, and performance evaluation theory, as well as continuing to study how risk, deterrence, and resilience concepts are leveraged to support antiterrorism efforts, academics and practitioners might flesh out a framework for a logic model or other performance- evaluation approach that integrates these concepts to help evaluate performance for agencies with a terrorism prevention/deterrence mission.

One might conjecture that an effort to build a performance- evaluation framework based on quantitative risk metrics might get at the historical differentiation between performance budgeting and program budgeting. The former, derived from scientific management principles, was considered a different budgeting system from the latter, influenced by economic and systems analysis.[53] If program objectives are to reduce risk and minimize residual risk, and quantitative risk reduction is a metric, perhaps both performance and program-based budgeting are simultaneously attainable by one agency. One might also speculate that such a framework could integrate both the input accountability concerns and the outcome-based performance concerns that Heinrich proposes:

> *[a]n important question that arises for public managers and researchers is, are outcome-based performance management systems more effective than traditional approaches to bureaucratic control?*[54]

In addition to the constraints identified earlier, Caudle claims establishing cause and effect relationships to guide measurement techniques for homeland security programs is still nascent.[55] With the knowledge that perfectly quantifiable metrics may not be realistic, an agency can still move forward with studying correlation between activities and risk reduction/residual risk metrics for antiterrorism programs. Collins advocates that the public sector should not focus exclusively on "perfectly quantifiable metrics," but should at least gather evidence of progress.[56]

Risk reduction is a quantifiable metric, but correlating costs of assets to execute risk-reduction activities may get at the challenge that Lewis posed in his seminal work on public budgeting. If we subscribe to the theory of evaluating budgets based on marginal utility, maximum gain for expenditures can only be obtained if those expenditures are distributed amongst different purposes such that the last dollar spent for each purpose yields the same return.[57] The concept of marginal utility entails analysis of how alternative uses of the same increment of available resources would yield different returns on investment, and prioritizing those alternative uses.[58]

Some agencies with antiterrorism missions may focus on control-based budgeting and track expenditures for assets, such as boats and aircraft. If the outcomes to be achieved are risk-reduction measures that can be sliced/diced in different ways, marginal utility theory may mean those agencies can link expenditures to risk reduced through threat reduction alone, through vulnerability reduction, through consequence reduction, or permutations of the above. This portfolio of options may have implications for how such agencies defend their budgets, per marginal utility theory, in an incremental budgetary environment.

Proposed Way Ahead

The next steps to continue this framework development effort might entail the following.

1. Flesh out a notional logic model that links agency antiterrorism activities, such as port patrols and vessel escorts, to agency accomplishments (possibly reduced risk), to agency outcomes (possibly residual risk).
2. Hypothesize appropriate metrics for each activity, accomplishment, and outcome. Consider direct and indirect or "proxy" metrics.
3. Assess whether those metrics might be modified to accommodate different budgeting theories (line item/responsibility center, efficiency, effectiveness).
4. Assess whether metrics can accommodate quantifiable deterrence/adaptive adversary considerations, network- exploitation susceptibility and other network effects on vulnerability, and/or network effects on consequence and resilience.
5. Assess the "aggregatibility" and "severability" of various metrics. For example, with respect to adaptive adversary factors, assess whether metrics derived from the concept of attacker and defender "utility" should segregate from those metrics, or aggregate therein, costs and other agency resource inputs to execute antiterrorism activities.

6. Assess the effects of other organizations with similar missions upon the efficacy of certain metrics in evaluating logic-model elements.
7. Assess whether a linear “pipeline” model, “outcome-chain”, recursive loop model, “realist” model, or other variety of logic model is most preferable.
8. Socialize various logic model formats/details with program sponsors, budget analysts, and agency overseers and revise models as appropriate.
9. Determine whether the preferred model would meet the threshold for formal agency verification, validation, and accreditation efforts, and estimate needed resources if that determination is in the affirmative.

Ongoing efforts to develop agency performance evaluation frameworks should be assessed as part of this way ahead.

Appendix

Here, we show some basic logic models that broach the recommended steps in the Proposed Way Ahead. These are not intended to be exhaustive, but instead are intended to illustrate, at a high level, how the concepts discussed in this essay might be presented for further exploration.

Threat Reduction

Logic Model Explanation

First, we show a notional activity-accomplishment-outcome logic model for deterrence activities (threat reduction). We show notional metrics, partitioned by the three budgeting theories: line item or cost center, efficiency, and effectiveness.

Purpose: Deterrence

Activity		Metric
Stationary Target	"Zone Defense"	# Activities / time or $ expended
Moving Target	"Point Defense"	
Stationary Target	"Point Defense"	

Accomplishment	Metric		
Attacks Deterred	Line Item	Efficiency	Effectiveness
	$T\downarrow$	$\frac{R\downarrow\vert_{T\downarrow}}{\$,time}$	$R\downarrow\vert_{T\downarrow}$

Outcome	Metric		
Residual Threat	Line Item	Efficiency	Effectiveness
	T_{res}	$\frac{R_{res}\vert_{T\downarrow}}{\$,time}$	$R_{res}\vert_{T\downarrow}$

(https://www.hsaj.org/resources/uploads/2018/12/Risk-Based_Performance_Metrics_figure1.1.png)

Figure 1. Logic model, deterrence activities (threat reduction)

Key:

$T\downarrow$ = threat reduced (as per deterrence activities)

$\frac{R\downarrow\vert_{T\downarrow}}{\$,time}$ = risk reduced given threat reduced, divided by resource inputs (time and/or money)

$R\downarrow\vert_{T\downarrow}$ = risk reduced given threat reduced, irrespective of resource inputs

T_{res} = residual threat (after deterrence activities executed)

$\frac{R_{res}\big|_{T\downarrow}}{\$, time}$ = residual risk given threat reduced, divided by resource inputs (time and/or money)

$R_{res}\big|_{T\downarrow}$ = residual risk given threat reduced, irrespective of resource inputs

In Figure 1, activities such as stationary and moving target defenses can be measured by number of activities performed, per resource input such as time or money, or both. The accomplishment of this effort is attacks deterred, with possible metrics of threat reduced (line item – tie to specific activity or asset performing activity), risk reduced as a function of threat per resource input (efficiency), or risk reduced as a function of threat (effectiveness). The outcome is residual risk, or what risk remains to the infrastructure after deterrence activities are executed.

Analysis

Here, if risk reduction is used as an efficiency or effectiveness metric, it could be isolated to the risk reduced solely as a function of threat-reducing or "deterrence" activities noted. The classic risk equation also incorporates vulnerability (V) and consequence (C) terms.

$$R = f(T, V, C)$$

Eq. 1. Basic Risk Equation

In reality, do security activities simultaneously reduce more than one element of the risk equation? This gets into aggregatibility/severability challenges, but specific to threat reduction efforts, the double-counting effects of quantifiable deterrence discussed in Taquechel and Lewis (2012) may be a consideration in performance measurement.

Double Counting Threat Reduction

One can argue that change in threat, or attacker capability and intent to attack, is a function of changes in target vulnerability and/or consequence.

$$T = f(V, C)$$

Eq. 2. Threat as function of vulnerability, consequence

We also know that threat is derived from intent and capability:

$$T = f(Intent, Cap)$$

Eq. 3. Threat as function of intent, capability

Previous work[59] has proposed that intent is a function of a ratio of attacker expected utility (UeA), or benefit from a successful attack, to the aggregate of all expected utilities from available attacker courses of action:

$$Intent = \frac{U_e A}{\sum U_e A}$$

Eq. 4. Intent as function of attacker expected utility

We also can surmise that attacker expected utility is a function of target vulnerability and consequence. What a target's defender stands to lose, an attacker stands to gain:

$$U_e A = f(V, C)$$

Eq. 5. Attacker expected utility as function of vulnerability, consequence

How does this lead to double counting? If target V or C decreases due to the target defender's actions, expected utility of an attack would decrease, thus decreasing intent and attacker threat. This ultimately suggests risk reduction.

$$V\downarrow, C\downarrow \rightarrow U_e A\downarrow \rightarrow Intent\downarrow \rightarrow T\downarrow \rightarrow R\downarrow$$

However, the effect of vulnerability and/or consequence reduction itself should be sufficient to argue risk is reduced:

$$V\downarrow, C\downarrow \rightarrow R\downarrow$$

Therefore, isolating the effects of threat reduction due to deterrence-oriented activities upon risk reduction becomes theoretically challenging. Did the risk reduce because an adversary noticed the point or zone defense activities and therefore had less intent to act? If so, by that logic, risk would be mathematically reduced twice: by the lowering of threat (per Equation 3), and the lowering of vulnerability or consequence (per Equation 1). While we can argue on a theoretical level that this double-counting effect of deterrence activities seems logical, from a performance metrics standpoint, one challenge may be arguing how much risk reduction is directly attributable to activities intended to deter, or reduce threat. Zone defense security activities seem more susceptible to this challenge, if they do not focus security coverage on individual targets, but instead cast a wide net over a group of targets. The effort to reduce target vulnerability with a randomized, "zone defense" presence may be less effective than the effort to reduce attacker intent to attack, and thus reduce threat. The relationship between specific tactical activities and metrics must be explored further.

Tracking Expenditures

The nexus between agency expenditure of time and/or money obligated to execute these deterrence-oriented activities, and the execution of the activities themselves, must be clear in order to have defensible efficiency metrics. For instance, if the funding for assets executing deterrence activities is earmarked specifically for those activities, but then the asset is diverted to perform a different task, the actual expenditure of those funds may trace to multiple activities in the accounting. This may make budget planning challenging if we link strategic-mission budgeting, mission-operational planning, and mission-execution activities.

Instead, budgeting to line-item capabilities (such as aircraft or boats) that perform multiple missions within an agency's portfolio may be easier, at least from a cost center/line-item budgeting perspective. Assets are constrained by engineering-driven costs such as fuel consumption and repair cycles, which may mean mission execution is constrained by available logistical-support funding. This may reflect realities of budgetary and logistical constraints, and whether outcome-based budgeting is feasible, especially in a prevention or deterrence-oriented mission, is subject to debate. This issue is particularly relevant to deterrence-focused activities in a logic model as they may be perceived as "generalist" in nature, not protecting any specific target nor responding to specific events or actionable intelligence.

Vulnerability Reduction

Next, we show a notional activity-accomplishment-outcome logic model for Prevention/Protection-oriented activities (vulnerability reduction) with notional metrics.

Purpose: Prevent & Protect

Activity		Metric
Stationary Target	"Zone Defense"	# Activities / time or $ expended
Moving Target	"Point Defense"	
Stationary Target	"Point Defense"	
Compliance Inspections		

Accomplishment	Metric		
	Line Item	Efficiency	Effectiveness
Attacks Prevented	$V\downarrow$	$\frac{R\downarrow\big\vert_{V\downarrow}}{\$,time}$	$R\downarrow\big\vert_{V\downarrow}$
Compliance Achieved			

Outcome	Metric		
	Line Item	Efficiency	Effectiveness
Residual Vulnerability	V_{res}	$\frac{R_{res}\big\vert_{V\downarrow}}{\$,time}$	$R_{res}\big\vert_{V\downarrow}$

(https://www.hsaj.org/resources/uploads/2018/12/Risk-Based_Performance_Metrics_figure2.1.png)

Figure 2. Logic model, prevention/protection activities (vulnerability reduction)

Key:

$V\downarrow$ = vulnerability reduced (as per prevent/protect activities)

$\frac{R\downarrow\big\vert_{V\downarrow}}{\$,time}$ = risk reduced given vulnerability reduced, divided by resource inputs (time and/or money)

$R\downarrow\big\vert_{v\downarrow}$ = risk reduced given vulnerability reduced, irrespective of resource inputs

V_{res} = residual vulnerability (after prevent/protect activities executed)

$\frac{R_{res}\big|_{V\downarrow}}{\$, time}$ = residual risk given vulnerability reduced, divided by resource inputs (time and/or money)

$R_{res}\big|_{V\downarrow}$ = residual risk given vulnerability reduced, irrespective of resource inputs

Logic Model Explanation

The first change from Figure 1 is that a new activity is introduced: compliance inspections. These inspections may be conducted armed or unarmed, depending on the purpose, but arguably armed inspections might prevent or protect against an imminent attack more effectively.

That notwithstanding, the next change is that one accomplishment is “attacks prevented” rather than “attacks deterred.” We introduce a second objective, “compliance achieved.” Whether this is synonymous with “attacks prevented” for logic-model analysis purposes may require additional examination.

Then, we see the outcome is “residual vulnerability,” or the probability of a successful attack given preventive/protective activities have been executed. The metrics for all activities, accomplishments, and outcomes in this logic model have the same structure as those in Figure 1, but are modified replacing Threat with Vulnerability.

Analysis

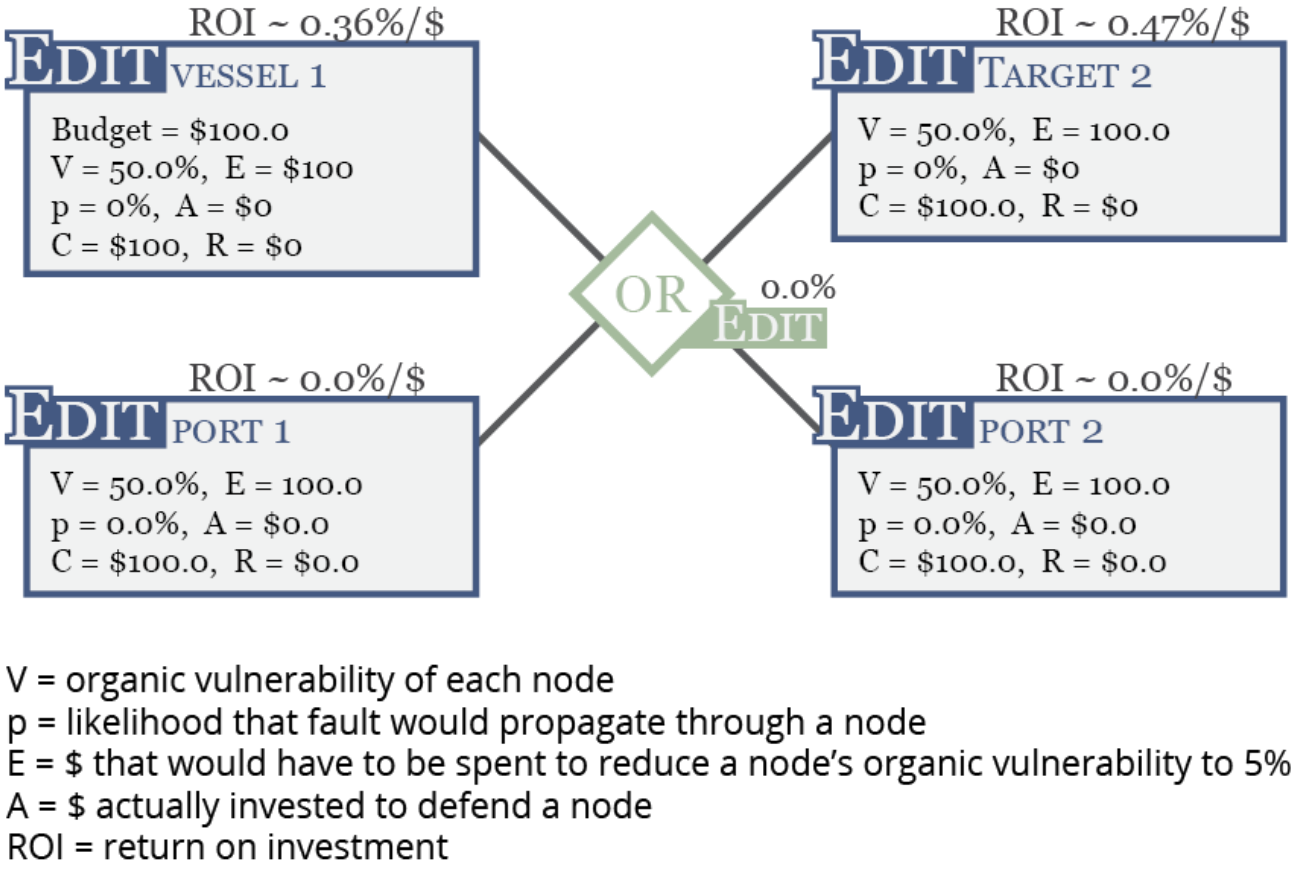
Aggregatibility/Severability

Since we are not focusing on the “double-counting” phenomenon here, aggregatibility and severability takes on a different meaning. Previous work has explored network effects in defending critical infrastructure.

Network Effects- V Reduction

We now lay the foundation for a modification to the Figure 2 logic model. This incorporates ideas from network analysis, with specific reference to the type of threat addressed. Are we protecting individual CIKR from direct attack, or from exploitation (moving illicit material through enroute to a different destination)? This analysis will assume the latter.

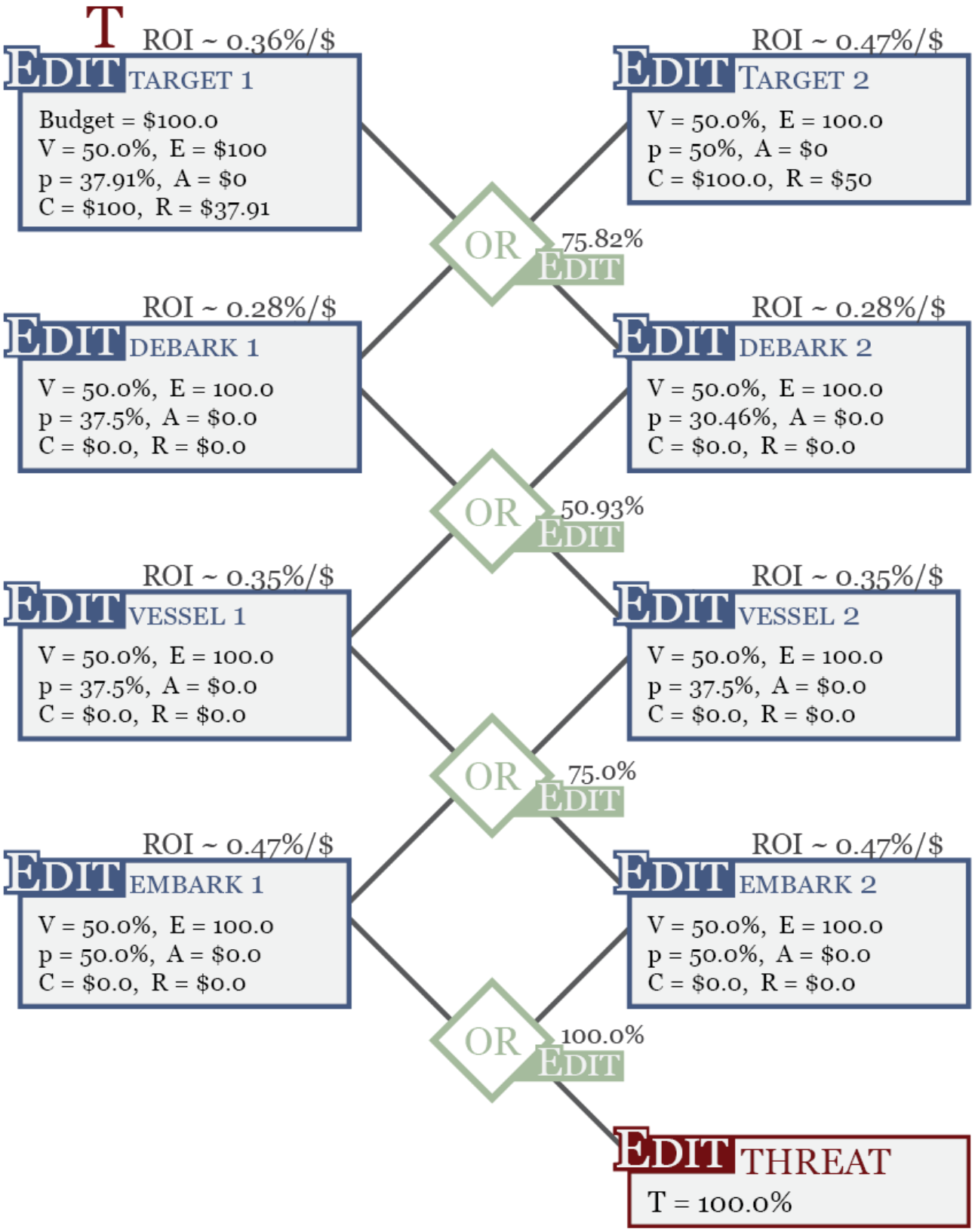
First, we discuss some basic concepts underpinning the “exploitation susceptibility” lens through which we will view network effects on vulnerability and performance metrics.



(https://www.hsaj.org/resources/uploads/2018/12/Figure_03.png)

Figure 3. Logic graph rendering of a transfer network – two ports and two vessels (Taquechel, 2010, p. 31)

A transfer network is a representation of how the terrorist-transfer threat, or movement of terrorists or illicit material, can propagate throughout transportation nodes.[60] If ports include CIKR that we prevent or protect against attacks, this network logic could be useful in exploring appropriate vulnerability reduction metrics for the transfer threat. Shown in expanded form, we have a notional network where an adversary might exploit foreign ports (embark), vessels, and domestic U.S. ports (debark), with the option to choose from multiple targets of attack:



(https://www.hsaj.org/resources/uploads/2018/12/Figure_04.png)

Figure 4. Logic graph rendering of an expanded transfer network (Taquechel, 2010, p. 32)

If our objective is to reduce “exploitation susceptibility,” or a specific type of vulnerability that estimates a port facility’s likelihood of exploitation due to an adversary moving illicit goods through undetected (rather than a direct attack against that facility), then our V metrics may take a different form for logic models. Previous work allows us to propose such a functional form of exploitation susceptibility:

$$V_{network} = 1 - \left(1 - V_{D1}\right)\left(1 - V_{D2}\right)$$

Eq. 6. Network vulnerability (exploitation susceptibility), transfer network as shown in Fig 4.

Here, this network exploitation susceptibility reflects the choices the attacker can make for target selection, and the VD1 / VD2 terms reflect a “nestled” vulnerability component that accounts for the ease with which attackers can move materiel or people through this network.

This equation may yield a different value for the network’s aggregate vulnerability, or aggregate exploitation susceptibility, than if we only consider the vulnerability of individual CIKR. We can protect infrastructure in the two “ports of debarkation,” but if our objective is to defend against network exploitation, our logic model metrics now take a different form:

Purpose: Prevent & Protect – Network Exploitation

Activity		Metric
Stationary Target	"Zone Defense"	# Activities / time or $ expended
Moving Target	"Point Defense"	
Stationary Target	"Point Defense"	
Compliance Inspections		

Accomplishment	Metric		
	Line Item	Efficiency	Effectiveness
Exploitation Prevented Compliance Achieved	$V_{network}\downarrow$	$\frac{R_{network}\downarrow\big\vert_{V_{network}\downarrow}}{\$, time}$	$R_{network}\downarrow\big\vert_{V_{network}\downarrow}$

Outcome	Metric		
	Line Item	Efficiency	Effectiveness
Residual Network Vulnerability (Exploitation Susceptibility)	$V^{res}_{network}$	$\frac{R^{res}_{network}\big\vert_{V^{res}_{network}\downarrow}}{\$, time}$	$R^{res}_{network}\big\vert_{V^{res}_{network}\downarrow}$

(https://www.hsaj.org/resources/uploads/2018/12/Risk-Based_Performance_Metrics_figure5.1.png)

Figure 5. Logic model, prevention/protection activities (network exploitation)

Key:

$V_{network}\downarrow$ = network exploitation susceptibility reduced (as per prevent/protect activities)

$\frac{R_{network}\downarrow\big\vert_{V_{network}\downarrow}}{\$, time}$ = network risk reduced given network exploitation susceptibility reduced, divided by resource inputs (time and/or money)

$R_{network}\downarrow\big\vert_{V_{network}\downarrow}$ = network risk reduced given network exploitation susceptibility reduced, irrespective of resource inputs

$V_{network}^{res}$ = residual network exploitation susceptibility (after prevent/protect activities executed)

$\frac{R_{network}^{res}\big|_{V_{network}^{res}\downarrow}}{\$, time}$ = residual network risk given network exploitation susceptibility reduced, divided by resource input (time and/or money)

$\frac{R_{network}^{res}\big|_{V_{network}^{res}\downarrow}}{\$, time}$ = residual network risk given network exploitation susceptibility reduced, irrespective of resource inputs

How is residual network exploitation susceptibility expressed? We add exponential terms to Equation 6 to account for modeled investments to reduce this susceptibility, expressed probabilistically.

$$V_{network}^{res} = 1 - \left(1 - V_{D1} e^{\left(\frac{-A_{D1}\lambda_{D1}}{E_{D1}}\right)}\right)\left(1 - V_{D2} e^{\left(\frac{-A_{D2}\lambda_{D2}}{E_{D2}}\right)}\right)$$

(https://www.hsaj.org/resources/uploads/2018/12/Eq7.png)

Eq. 7. Network vulnerability (exploitation susceptibility), residual after investment

Importantly – the focus of the prevention/protection activities in this logic model remains the same CIKR targets as in Figure 3 –US port infrastructure. But, there are additional influences on the vulnerability that those executing these activities "inherit" from upstream defensive efforts, such as overseas compliance inspections. These influences may be outside the scope of the logic model under consideration.

Furthermore, the compliance inspection activity holds yet another vulnerability-reduction purpose when the objective is specifically to prevent or protect against exploitation via nuclear weapons shipments. This may entail inspection of weapon-detection equipment and SOP compliance efforts. See Taquechel, Hollan and Lewis (2015) for more discussion.

Tracking Expenditures – Issues Specific to V-reducing Activities

One consideration for the efficiency metric denominator here is how realistic the influence of protective activities in U.S. ports is, when the issue at hand is exploitation susceptibility. The vulnerability-reduction effects of overseas compliance inspections and at-sea actions may influence exploitation susceptibility, and protection activities in U.S. ports may only contribute marginally to overall network-exploitation susceptibility reduction. This may be a return on investment consideration if the prevailing preference for performance metrics is driven by efficiency, or accomplishment per expenditure. This gets back to the theoretical consideration of external influences upon performance metrics as discussed in Rogers (2008).

Consequence Reduction

Next, we show a notional activity-accomplishment-outcome logic model for resilience-oriented activities (consequence reduction), with notional metrics.

Purpose: Resilience

Activity	Metric
Port Security Grants - Resilience Investment	Grants approved per input effort/ (Time to process, $)

Accomplishment	Metric		
Economic Loss Reduced	Line Item	Efficiency	Effectiveness
	$C_{\$} \downarrow$	$\frac{R_{C_{\$}} \downarrow \big\vert_{C_{\$}\downarrow}}{\$, time}$	$R_{C_{\$}} \downarrow \big\vert_{C_{\$}\downarrow}$

Outcome	Metric		
Economic Productivity Retained	Line Item	Efficiency	Effectiveness
	$C_{\$}^{res}$	$\frac{R^{res}_{c_{\$}} \big\vert_{C_{\$}\downarrow}}{\$, time}$	$R^{res}_{c_{\$}} \big\vert_{C_{\$}\downarrow}$

(https://www.hsaj.org/resources/uploads/2018/12/Risk-Based_Performance_Metrics_figure6.1.png)

Figure 6. Logic model, resilience activities (consequence reduction)

Key:

$C_{\$}\downarrow$ = economic loss theoretically avoided (by resilience activities)

$\frac{R_{C_{\$}}\downarrow|_{C_{\$}\downarrow}}{\$, time}$ = CIKR lost productivity avoided given resilience activities, accounting for probability of attack, divided by resource inputs (time and/or money)

$R_{C\$}\downarrow|_{C_{\$}\downarrow}$ = CIKR lost productivity avoided, irrespective of resource inputs

$C_{\$}^{res}$ = residual economic productivity (after resilience activities executed)

$\frac{R^{res}_{c_{\$}}|_{C_{\$}\downarrow}}{\$, time}$ = residual CIKR productivity, accounting for probability of attack, divided by resource input (time and/or money)

$R^{res}_{c_{\$}}|_{C_{\$}\downarrow}$ = residual CIKR productivity, irrespective of resource inputs

Logic Model Explanation

Here, the activity is port security grants, which per previous work were proposed to take a resilience-focused approach, providing to CIKR money specifically earmarked for capability to rebuild to facilitate some level of productivity after an incident. See Taquechel (2013) for more details.

The accomplishment is economic loss theoretically reduced or avoided by these resilience activities, as lost economic productivity can be considered a consequence. Metrics entail quantified economic loss (line item), or risk as a function of that economic consequence (network lost productivity that accounts for probability of attack), either per effort expended to administer grants (efficiency), or disregarding effort (effectiveness).

The outcome is residual economic productivity, measured by dollars (line item), or by residual network functionality per grant administration effort, or without regard to effort (efficiency vs effectiveness).

Analysis

Aggregatibility/Severability

Here, aggregatibility/severability of metrics also gets into network effects, but in terms of "cascading economic effects" on networks of infrastructure, as explored in Taquechel (2013). In other words, the aggregatibility focuses on the network effects of consequence rather than the network effects of vulnerability or exploitation susceptibility. We can call this "failure susceptibility" in consequence terms.

Network Effects- C Reduction (Resilience)

We now show a modification to the Figure 6 logic model. This incorporates ideas from network theory with a consequence focus. Taquechel (2013) introduced the term "inherited failure susceptibility," proxied by CIKR network node degree, meaning the number of upstream suppliers a CIKR has in a supply chain. When considered in tandem with a CIKR's organic failure susceptibility, e.g. lack of reserve raw product onsite to resume production after a disruption, inherited failure susceptibility may exacerbate overall network failure susceptibility.

To set context for the updated logic model, we introduce an "expected network consequence" term:

$$Con^{1(\exp)} = \sum_{i} \left(g_i Con_i^{(\max)} e^{\left(\frac{-A_i^{raw} \lambda_i^{raw}}{E_i^{raw}} \right)} \right)$$

(https://www.hsaj.org/resources/uploads/2018/12/Risk-Based_Performance_Metrics_Eq8.png)

Eq. 8. Expected consequence of lth supply chain network with i nodes

This term accounts for the organic failure susceptibility of all nodes in a supply chain network. The organic failure susceptibility is modeled as an exponential relationship between resilience effort actually invested and investment needed to minimize failure susceptibility. This susceptibility modifies

probabilistically the maximum possible economic loss to an ith node $Con_i^{(max)}$. The expected consequence to each node sums to the total expected network consequence.

If resilience activities covered in the logic model only improve resilience at some of the network nodes, they may reduce overall network failure susceptibility and economic loss, but the interdependencies between network nodes, proxied by node degree g, may increase potential loss. That said, we want to expand our depiction of network expected consequence, as a function of resilience investments at the supplier nodes, here with maximum consequence $Con_s^{(max)}$.

$$Con^{1(\exp)} = \sum_i \left(\begin{array}{l} g_s Con_s^{(\max)} \left[\begin{array}{l} e^{\left(\frac{-A_s^{reb} \lambda_s^{reb}}{E_s^{reb}} \right)} \left(1 - e^{\left(\frac{-A_s^{raw} \lambda_s^{raw}}{E_s^{raw}} \right)} e^{\left(\frac{-A_s^{red} \lambda_s^{red}}{E_s^{red}} \right)} \right) \\ + \left(e^{\left(\frac{-A_s^{raw} \lambda_s^{raw}}{E_s^{raw}} \right)} e^{\left(\frac{-A_s^{red} \lambda_s^{red}}{E_s^{red}} \right)} \right) \end{array} \right] \\ + \sum_{I_j=3} g_{I_j} Con_{I_j}^{(\max)} e^{\left(\frac{-A_{I_j}^{raw} \lambda_{I_j}^{raw}}{E_{I_j}^{raw}} \right)} \\ + \sum_{C_k=6} g_{C_k} Con_{C_k}^{(\max)} e^{\left(\frac{-A_{C_k}^{raw} \lambda_{C_k}^{raw}}{E_{C_k}^{raw}} \right)} \end{array} \right)$$

(https://www.hsaj.org/resources/uploads/2018/12/Risk-Based_Performance_Metrics_Eq9.png)

Eq. 9. Expected consequence to lth supply chain network, expanded to show supplier-node failure probabilities

If we invest to increase the probability of rebuilding after a disruption, the A_s^{reb} term will increase, thus increasing economic productivity.

Next, we introduce a term for risk to a network, that factors in network expected consequence:

$$R^{l}_{cond} = Cap^{l}_{s} V^{l}_{s} Con^{l(\exp)}$$

Eq. 10. Conditional risk to lth supply chain network

The risk to a supply chain network is thus a function of network expected consequence, but also of an attacker's capability to attack supplier node s, and that node's vulnerability to attack. Therefore, an efficiency metric would be conditional network risk reduced or avoided, as a function of possible economic loss reduced, per effort to ensure such loss reduction. This term can capture the expanded form of expected consequence shown in Equation 9, to allow simulation of resilience investments that would lower conditional risk, retaining economic productivity. This retained economic productivity can be expressed as a resilience term, the difference between maximum pre-disruption economic output, and conditional risk (expected economic loss) resulting from a disruption:

$$\mathrm{Re}\,silience^{l} = Con^{l(\max)} - R^{l}_{cond}\Big|_{Con^{l(\exp)}\downarrow}$$

(https://www.hsaj.org/resources/uploads/2018/12/Risk-Based_Performance_Metrics_Eq11.png)

Eq. 11. Resilience of lth supply chain, given efforts to reduce expected economic loss

Therefore, we can now show our modification to Figure 6:

Purpose: Resilience – Network

Activity	Metric
Port Security Grants - Resilience Investment	Grants approved per input effort/ (Time to process, $)

Accomplishment	Metric
Network Economic Loss Reduced	Line Item: $Con^{1(\exp)}\downarrow$ Efficiency: $\frac{R^{l}_{cond}\downarrow\big\vert_{Con^{1(\exp)}\downarrow}}{\$, time}$ Effectiveness: $R^{l}_{cond}\downarrow\big\vert_{Con^{1(\exp)}\downarrow}$

Outcome	Metric
Economic Productivity Retained	Line Item: $Con^{1(\exp)}$ Efficiency: $\frac{Con^{1(\max)} - R^{l}_{cond}\big\vert_{Con^{l(\exp)}\downarrow}}{\$, time}$ Effectiveness: $Con^{1(\max)} - R^{l}_{cond}\big\vert_{Con^{l(\exp)}\downarrow}$

(https://www.hsaj.org/resources/uploads/2018/12/Risk-Based_Performance_Metrics_figure7.1.png)

Figure 7. Logic model, resilience activities (consequence reduction) – NETWORK EFFECTS

Key:

$Con^{1(\exp)}\downarrow$ = **expected supply chain** economic loss theoretically avoided (by resilience activities)

$\frac{R^{l}_{cond}\downarrow\big\vert_{Con^{1(\exp)}\downarrow}}{\$, time}$ = **supply chain** lost productivity avoided given resilience activities, accounting for probability of attack, divided by resource inputs (time and/or money)

$R^{l}_{cond}\downarrow\big\vert_{Con^{1(\exp)}\downarrow}$ = **supply chain** lost productivity avoided, irrespective of resource inputs

$Con^{1(\exp)}$ = residual **supply chain** economic productivity (after resilience activities executed)

$\frac{Con^{1(\max)} - R_{cond}^{l}\Big|_{Con^{l(\exp)}\downarrow}}{\$, time}$ = residual **supply chain** productivity, accounting for probability of attack, divided by resource inputs (time and/or money)

$Con^{1(\max)} - R_{cond}^{l}\Big|_{Con^{l(\exp)}\downarrow}$ = residual **supply chain** productivity, irrespective of resource inputs

Tracking Expenditures – Issues Specific to C-reducing Activities

As with vulnerability-reduction efforts, the inputs to achieve consequence reduction, if applied only at certain infrastructure in a network, must be considered relative to the proportional effect of those reduction efforts. More specifically, if port security grants increase resilience by lowering expected economic loss at supplier nodes (for example, in a port), but the supply-chain network is composed of downstream nodes with high organic failure susceptibility, the efforts to increase port facility resilience may have a minimal effect on overall supply chain resilience. If much effort is expended to administer port security grants, that may not be an ideal return on investment. However, efficiency metrics may not be the prevailing budgetary theory preference.

About the Authors

Eric F. Taquechel is a U.S. Coast Guard officer with experience in shipboard operations, port operations, critical infrastructure risk analysis, contingency planning/force readiness, operations analysis, planning, programming, budgeting, and execution process support. He has authored and co-authored various publications on risk, resilience, and deterrence in *HSAJ*, the *Journal of Homeland Security and Emergency Management*, and *IEEE*. Most recently he and a coauthor published "A Right-Brained Approach to Critical Infrastructure Protection Theory in Support of Strategy and Education: Deterrence, Networks, and Antifragility", which was selected as a Best Paper presented at the CHDS's 2017 University-Academic Partnership Initiative's 10th Annual Homeland Defense and Security Education Summit. Taquechel has taught courses on critical infrastructure protection and is a FEMA Master Exercise Practitioner. He holds a MPA from Old Dominion University, a master's degree in Security Studies from the Naval Postgraduate School, and a BS from the U.S. Coast Guard Academy. Taquechel (corresponding author) may be contacted at etaqu001@odu.edu (mailto:etaqu001@odu.edu).

Dr. Marina Saitgalina is an Assistant Professor at the School of Public Service at Old Dominion University. Previously, she was an Assistant Professor at Oakland University, Michigan. Her areas of research include public administration, nonprofit management, nonprofit-government collaborations, and emergency management. She has multiple publications on such topics as nonprofit collaborations and institutional theories, and public management in emergencies in *Public Management Review*, *Administration & Society*, and *Journal of Public and Nonprofit Affairs* among others. She holds her MPA degree from the Academy of Public Administration in Russia, and a Ph.D. in Public Administration and Management from University of North Texas. Saitgalina may be contacted at msaitgal@odu.edu (mailto:msaitgal@odu.edu).

Acknowledgements

The authors wish to thank the referees who helped improve the quality of this work.

Disclaimer

The original opinions and recommendations in this work are those of the authors and are not intended to reflect the positions or policies of any government agency.

Notes

1 Carolyn J. Heinrich, "Outcomes–Based Performance Management in the Public Sector: Implications for Government Accountability and Effectiveness," *Public Administration Review* 62(2002): 712-725.

2 Theodore H. Poister, Obed Q. Pasha, and Lauren H. Edwards, "Does Performance Management Lead to Better Outcomes? Evidence from the U.S. Public Transit Industry," *Public Administration Review 73*(2013): 625-636.

3 U. S. Department of Homeland Security, *DHS Risk Lexicon* (2010), https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf (https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf), Web accessed March 26, 2018.

4 Ibid.

5 Ibid.

6 Theodore H. Poister, Obed Q. Pasha, and Lauren H. Edwards, “Does Performance Management Lead to Better Outcomes? Evidence from the U.S. Public Transit Industry,” 625-636.

7 Janet V. Denhardt and Robert B. Denhardt, *The New Public Service: Serving, Not Steering* (4th ed.) (New York: Routledge, 2015).

8 Kathryn Newcomer and Sharon Caudle, “Public Performance Management Systems: Embedding Practices for Improved Success,” *Public Performance & Management Review* 35(2011): 108-132.

9 Yilin Hou, “Budgeting for Fiscal Stability over the Business Cycle: A Countercyclical Fiscal Policy and the Multiyear Perspective on Budgeting,” *Public Administration Review* 66(2006): 730-741.

10 Allen Schick, “The Road to PPB: The Stages of Budget Reform,” *Public Administration Review* 26(1966): 243–258.

11 Yilin Hou, “Budgeting for Fiscal Stability over the Business Cycle: A Countercyclical Fiscal Policy and the Multiyear Perspective on Budgeting.”

12 Ibid.

13 Department of Homeland Security, Performance Budget Overview, FY2006 Congressional Budget Justification, https://www.dhs.gov/xlibrary/assets/Budget_PBO_FY2006.pdf (https://www.dhs.gov/xlibrary/assets/Budget_PBO_FY2006.pdf), Web accessed May 30, 2018.

14 Kathryn Newcomer and Sharon Caudle, “Public Performance Management Systems: Embedding Practices for Improved Success.”

15 Thomas M. Rabovsky, “Using Data to Manage for Performance at Public Universities,” *Public Administration Review* 74(2014): 260-272.

16 John A. McLaughlin and Gretchen B. Jordan, “Logic Models: A Tool for Telling your Program’s Performance Story,” *Evaluation and Program Planning* 22(1999): 65-72.

17 Victoria A. Greenfield, Valeria L. Williams, and Elisa Eiseman, “Using Logic Models for Strategic Planning and Evaluation: Application to the National Center for Injury Prevention and Control,” RAND report (2006), https://www.rand.org/pubs/technical_reports/TR370.html (https://www.rand.org/pubs/technical_reports/TR370.html), Web accessed March 26, 2018.

18 Ibid.

19 See: Eric F. Taquechel, "Layered Defense: Modeling Terrorist Transfer Threat Networks and Optimizing Network Risk Reduction," *IEEE Magazine 24*(2010): 30-35; Eric F. Taquechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk," *Homeland Security Affairs* 8(August 2012), https://www.hsaj.org/articles/226 (https://www.hsaj.org/articles/226). Web accessed March 26, 2018; Eric F. Taquechel, "Options and Challenges of a Resilience-Based, Network-Focused Port Security Grant Program," *Journal of Homeland Security and Emergency Management 10*(2013): 521-554; Eric F. Taquechel, Ian Hollan, and Ted G. Lewis, "Measuring the Deterrence Value of Securing Maritime Supply Chains against WMD Transfer and Measuring Subsequent WMD Risk Reduction," *Homeland Security Affairs 11*(February 2015), https://www.hsaj.org/articles/1304 (https://www.hsaj.org/articles/1304), Web accessed March 26, 2018;

Eric F. Taquechel and Ted G. Lewis, "More Options for Quantifying Deterrence and Reducing Critical Infrastructure Risk: Cognitive Biases," *Homeland Security Affairs 12*(September 2016), https://www.hsaj.org/articles/12007 (https://www.hsaj.org/articles/12007), Web accessed March 26, 2018.

20 See: David L. Alderson, Gerald G. Brown, Matt Carlyle, and R. Kevin Wood, "Solving Defender-Attacker-Defender Models for Infrastructure Defense," *Proceedings of the 12th INFORMS Computing Society Conference: Research, Computing, and Homeland Defense* (2011): 28-49*;* Louis A. Cox, "Some Limitations of "Risk=Threat x Vulnerability x Consequence" for Risk Analysis of Terrorist Attacks," *Risk Analysis 28*(2008): 1749-1761; Nikhil S. Dighe, Jun Zhuang, and Vicki M. Bier, "Secrecy in Defensive Allocations as a Strategy for Achieving more Cost Effective Deterrence," *International Journal of Performability Engineering* 5 (2009): 31- 43; Erik Jenelius, Jonas Westin, and Åke J. Holmgren, "Critical Infrastructure Protection under Imperfect Attacker Perception," *International Journal of Critical Infrastructure Protection* 3 (2010): 16-26; Jerome Kahan, Andrew Allen, and Justin George, "An Operational Framework for Resilience," *Journal of Homeland Security and Emergency Management 6*(2009): 1-47; Richard N. Lebow and Janet G. Stein, "Rational Deterrence Theory: I Think, Therefore I Deter," *World Politics* 41 (1989): 208–224; Ted G. Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (Hoboken, NJ: Wiley Interscience, 2006); Ted G. Lewis, *Network Science: Theory and Applications* (Hoboken, NJ: Wiley Interscience, 2009); Andrew R. Morral and Brian A. Jackson, "Understanding the Role of Deterrence in Counterterrorism Security," RAND Occasional Paper (2009), http://www.rand.org/pubs/occasional_papers/OP281.html (http://www.rand.org/pubs/occasional_papers/OP281.html) Web accessed March 26, 2018; Eric D. Vugrin, Drake E. Warren, Mark A. Ehlen, & R. Chris Camphouse, "A Framework for Assessing the Resilience of Infrastructure and Economic Systems," in *Sustainable and Resilient Critical Infrastructure Systems: Simulation, Modeling, and Intelligent Engineering*, eds. Kasthurirangan Gopalakrishnan and Srinivas Peeta (New York: Springer, 2010), 77–116.

21 P. Cronin and A. Cronin, *Challenging Deterrence: Strategic Stability in the Twenty-First Century*, Changing Character of War Series, (Oxford: Oxford University Press, 2007), http://ccw.modhist.ox.ac.uk/events/archives/mt06_deterrence/deterrence_report_mt2006.pdf

(http://ccw.modhist.ox.ac.uk/events/archives/mt06_deterrence/deterrence_report_mt2006.pdf), Web accessed March 7, 2010.

22 U. S. Department of Homeland Security, *DHS Risk Lexicon* (2010), https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf (https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf), Web accessed March 26, 2018.

23 Eric F. Taquechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk," *Homeland Security Affairs* 8(August 2012), https://www.hsaj.org/articles/226 (https://www.hsaj.org/articles/226), Web accessed March 26, 2018.

24 Scott Savitz, Miriam Matthews, and Sarah Weilant, *Assessing Impact to Inform Decisions: A Toolkit on Measures for Policymakers,* RAND report (2017), https://www.rand.org/pubs/tools/TL263.html (https://www.rand.org/pubs/tools/TL263.html), Web accessed March 26, 2018.

25 Laurie M. Anderson et al., "Using Logic Models to Capture Complexity in Systematic Reviews," *Research Synthesis Methods 2*(2011): 33-42.

26 Patricia J. Rogers, "Using Programme Theory to Evaluate Complicated and Complex Aspects of Interventions," *Evaluation 14*(2008): 29-48.

27 Ibid.

28 U. S. Department of Homeland Security, *DHS Risk Lexicon* (2010), https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf (https://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf), Web accessed March 26, 2018.

29 Ted G. Lewis, *Network Science: Theory and Applications.*

30 Daniel Henstra, "Evaluating Local Government Emergency Management Programs: What Framework Should Public Managers Adopt?" *Public Administration Review 70*(2010): 236-246.

31 Susan Cutter, Christopher Burton, Christopher Emrich, "Disaster Resilience Indicators for Benchmarking Baseline Conditions," *Journal of Homeland Security and Emergency Management 7*(2010): 1-22.

32 Sue C. Funnell and Patricia J. Rogers, *Purposeful Program Theory: Effective Use of Theories of Change and Logic Models* (San Francisco: Jossey-Bass, 2011).

33 Anthony A. Braga and Brenda J. Bond, "Policing Crime and Disorder Hot Spots: A Randomized Controlled Trial," *Criminology 46*(2008): 577-607.

34 Astrid Brousselle and Francois Champagne, “Program Theory Evaluation: Logic Analysis,” *Evaluation and Program Planning 34*(2011): 69-78.

35 Anthony A. Braga and Brenda J. Bond, “Policing Crime and Disorder Hot Spots: A Randomized Controlled Trial,” *Criminology 46*(2008): 577-607.

36 Sean Nicholson-Crotty, Nick A. Theobald, Jill Nicholson-Crotty, “Disparate Measures: Public Managers and Performance-Measurement Strategies,” *Public Administration Review 66*(2006): 101-113.

37 Bilal M. Ayyub, “Systems Resilience for Multihazard Environments: Definition, Metrics and Valuation for Decision Making,” *Risk Analysis 34*(2014): 340-355.

38 Ralph L. Keeney and Detlof Von Winterfeldt, “A Value Model for Evaluating Homeland Security Decisions,” *Risk Analysis 31*(2011): 1470-1487.

39 Ibid.

40 Holly Hilliard, Gregory S. Parnell, and Edward A. Pohl, “Evaluating the Effectiveness of the GNDA using Multi-Objective Decision Analysis,” *Systems Engineering 18*(2015): 441-452.

41 Ibid.

42 Eric F. Taquechel and Ted G. Lewis, “How to Quantify Deterrence and Reduce Critical Infrastructure Risk (https://www.hsaj.org/articles/226).

43 Victoria A. Greenfield, Valeria L. Williams, and Elisa Eiseman, “Using Logic Models for Strategic Planning and Evaluation: Application to the National Center for Injury Prevention and Control. (https://www.rand.org/pubs/technical_reports/TR370.html)”

44 Ibid.

45 Sharon Caudle, “Homeland Security: Approaches to Results Management,” *Public Performance & Management Review 28*(2005): 352-375.

46 Sean Nicholson-Crotty, Nick A. Theobald, Jill Nicholson-Crotty, “Disparate Measures: Public Managers and Performance-Measurement Strategies.”

47 Suresh Cuganesan and David Lacey, “Developments in Public Sector Performance Measurement: A Project on Producing Return on Investment Metrics for Law Enforcement,” *Financial Accountability & Management 27*(2011): 458-479.

48 Robert D. Behn, "Why Measure Performance? Different Purposes Require Different Measures," *Public Administration Review 63*(2003): 586-606.

49 Ibid.

50 Victoria A. Greenfield, Valeria L. Williams, and Elisa Eiseman, "Using Logic Models for Strategic Planning and Evaluation: Application to the National Center for Injury Prevention and Control (https://www.rand.org/pubs/technical_reports/TR370.html)."

51 Scott Savitz, et al. , *Enhancing U.S. Coast Guard Metrics,* RAND report, 2015), https://www.rand.org/pubs/research_reports/RR1173.readonline.html (https://www.rand.org/pubs/research_reports/RR1173.readonline.html), Web accessed March 26, 2018.

52 Sharon Caudle, "Homeland Security: Approaches to Results Management," *Public Performance & Management Review 28*(2005): 352-375.

53 Allen Schick, "The Road to PPB: The Stages of Budget Reform."

54 Carolyn J. Heinrich, "Outcomes–Based Performance Management in the Public Sector: Implications for Government Accountability and Effectiveness," *Public Administration Review* 62(2002): 712-725.

55 Sharon Caudle, "Homeland Security: Approaches to Results Management."

56 James C. Collins, *Good to Great and the Social Sectors: A Monograph to Accompany Good to Great, (*Harper: New York, 2005).

57 Verne B. Lewis, "Toward a Theory of Budgeting," *Public Administration Review 12*(1952): 42-54.

58 Ibid.

59 Eric F. Taquechel and Ted G. Lewis, "How to Quantify Deterrence and Reduce Critical Infrastructure Risk (https://www.hsaj.org/articles/226)."

60 Eric F. Taquechel, "Layered Defense: Modeling Terrorist Transfer Threat Networks and Optimizing Network Risk Reduction."

More Articles

- Volume XIII (2017) (https://www.hsaj.org/articles/category/volume-xiii)
- Volume XII (2016) (https://www.hsaj.org/articles/category/volume-xii)
- Volume XI (2015) (https://www.hsaj.org/articles/category/volume-xi)
- CHDS Theses: Executive Summaries (https://www.hsaj.org/articles/category/chds-theses-executive-summaries)
- Archives (https://www.hsaj.org/archives)

FIND

CENTER FOR HOMELAND DEFENSE AND SECURITY
NAVAL POSTGRADUATE SCHOOL (http://www.chds.us)

FEMA (http://www.fema.gov/national-preparedness-directorate)